TASK ORDER

GST0011AJ0025 Mod 122

Enterprise Networked Services Support (ENSS)

in support of:

Department Of Homeland Security (DHS)

Issued to:

Northrop Grumman Systems Corporation
Cyber Solutions Division
7575 Colshire Drive
Mclean, VA 22101

Under

Alliant Contract# GS00Q09BGD0056

issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F St NW
Washington DC 20405

FEDSIM Project Number 10068HSM

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. In addition, the following applies:

C.1 BACKGROUND

C.1.1 PURPOSE

The purpose of this Task Order is to provide support for the continued operations, maintenance and evolution of Department of Homeland Security (DHS) networks. DHS networks are a Federal enterprise infrastructure for information sharing which extend existing US Government capabilities not only to the Department of Homeland Security and its components, but to other Federal government agencies, and to first responders at the state, local, and tribal levels**.**

C.1.2 BACKGROUND

Fundamental to achieving DHS's missions is the ability to communicate effectively among the members of the Department and among DHS's mission partners in other agencies and organizations. This capability is essential to share Homeland Security information at the appropriate level of classification, to inform assessments and initiate appropriate action. The DHS Headquarters Office of the Chief Information Officer (OCIO) currently operates, and participates in the governance of enterprise scale information infrastructures to enable solutions to these communications needs.

The network infrastructure environment managed by DHS Headquarters, which is used to deliver Enterprise Networked Services (ENS), is in a state of transformation. When the department stood up in 2003, the infrastructure it inherited comprised dozens of networks that had earlier been developed and managed independently by the previously separate agencies. Under recent "One DHS" policies, the DHS OCIO has established an initiative to merge and harmonize existing networks into "Enterprise Networked Service" offerings that will provide effective and efficient network services while saving considerable costs through common architecture, shared management, and leveraged investments.

Central to the infrastructure transformation program is the "OneNet" initiative. This initiative comprises network circuit provisioning orders established under the GSA NETWORX program to supply DHS with its communications connectivity. DHS has established connectivity for new facilities through the OneNet initiative and is migrating older existing connections from their legacy providers to OneNet. The anticipated benefits of the OneNet migration include reduced costs for network connectivity, maintenance and management; reduced security risk (fewer networks means fewer security vulnerability points); less network complexity, and centralized governance and standards. These benefits will facilitate interoperability, information sharing and the rapid delivery of new services and capabilities.

DHS has also epstablished a policy to consolidate its data centers at limited primary locations. As in the case of telecommunications, the previously separate constituent DHS agencies managed their own data centers independently. The consolidation initiative is delivering

consistent governance and the opportunity to leverage facility and operational investments to reduce costs and improve performance. Data center management has been outsourced to specialty vendors responsible for establishing, operating and maintaining them in response to the evolving requirements of the department. In the foreseeable future, there is also a potential for providing additional geographic diversity at one or two additional locations which are elsewhere in the United States.

These basic infrastructure resources provide some of the infrastructure elements required for the OCIO to offer an array of "Enterprise Networked Services" to the department's many system users. These services support administrative and management as well as critical mission functions in the department. Network services are currently sensitive, but unclassified, and offered at three levels of classification and typically comprise end user work stations, enterprise office applications, data stores, and application hosting, supported by connectivity to the central core, and managed network and security operations, as well as gateways to related networks operated by other agencies.

While these centralized service offerings are in place and further enhancements are in the implementation and planning stages, the degree to which DHS components are taking advantage of the Enterprise offerings varies both by the offering and by DHS component.

DHS Enterprise Networked Services supports the continued operations, maintenance and evolution of the Homeland Secure Data Network (HSDN) which operates at the SECRET level and the C-LAN which provides TOP SECRET/Sensitive Compartmented Information (TS/SCI) extensions to the Defense Intelligence Agency (DIA) provisioned Joint Worldwide Intelligence Communications System (JWICS). Future work includes the transition of the C-LAN to the evolving Homeland TS/SCI Network (HTSN), and the development of a new program called Homeland Secure Communications (HSC) that will consolidate secure voice and video communications into a centrally managed activity at both the SECRET and the TS/SCI levels.

The HSDN and the C-LAN/HTSN are managed by authorities which are delegated and administered jointly by the DHS Office of Intelligence and Analysis (I&A) and the DHS OCIO and the DHS I&A, under an organization known as the National Security Systems (NSS) Joint Program Management Office (JPMO), whose charter also includes HSC.

The HSDN is a high-speed data network enabling actionable intelligence data, at the SECRET level, to flow among federal, state and local law enforcement. HSDN helps to provide actionable intelligence to first responders at the Federal, State and Local levels. HSDN currently supports over 200 sites consisting of over 3,000 users and is projected to grow to 1,000 sites consisting of 15,000 users over the next seven (7) years. HSDN is implemented at most DHS components, at over 40 State and Local Fusion Centers (SLFCs), and in over 20 other Federal agencies; these numbers are ever-growing weekly. The SLFCs are federally-sponsored, federally-operated intelligence fusion organizations that are designed to serve the mission needs of first responders at the state, local, and tribal levels (it is possible that that within the period of performance, first responder organizations may eventually transcend the present need to be federally operated).

The C-LAN currently is a conglomeration of TS/SCI systems that DHS inherited when it was created from 22 Federal organizations in 2003. DHS is in the process of stabilizing the C-LAN (which has never had a single architecture as it was inherited from multiple organizations) into a single HTSN. DHS forecasts that at least three (3) years will be needed before C-LAN technically evolves into the envisioned HTSN. When completed, HTSN will streamline and modernize data capabilities to enhance data communications and collaboration within DHS and other federal agencies and organizations in the Intelligence Community (IC). Until the HTSN architecture is defined, designed, implemented, tested and deployed, the current baseline C-LAN must be maintained. The C-LAN provides TS/SCI level intelligence to the intelligence gathering arms of the Federal Government as well as to a very limited number of State, Local, and Tribal ICs such as certain major metropolitan police enforcement agencies. In all, C-LAN currently supports over 10 locations consisting of 3,500 users and is projected to grow to 100 sites consisting of 15,000 users over the next seven (7) years.

In the future, HSC is envisioned to become a new program of record that consolidates the planning, architecture, and implementation of secure voice and video communications into a centrally governed and managed activity. HSC will provide effective and efficient voice and video services while saving considerable costs through leveraging common architecture, design, shared management, and leveraged investments.

The continuing evolution and operation of the HSDN and C-LAN supports preventing and combating terrorism and is critical to the national security of the US. The HSDN and the C-LAN support the gathering, analysis, creation and dissemination of actionable intelligence among Federal, State and Local Intelligence community members, first responders, and mission partners. The HSDN and the C-LAN incorporate organizations in Federal, State and Local jurisdictions that share information and collaborate on that shared information. Data interoperability and information sharing across many jurisdictions is critical to combating the global war on terrorism (GWOT).

C.1.3 AGENCY MISSION

Homeland security is a widely distributed and diverse national enterprise. It is built on the ideas of Strengthening Security: protecting the United States and its people, vital interests, and way of life; Promoting Resilience: fostering individual, community, and system robustness, adaptability, and capacity for rapid recovery; and Facilitating Customs and Exchange: Expediting and enforcing lawful trade, travel, and immigration.

These concepts have led DHS to define its core mission set as:

1: Preventing Terrorism and Enhancing Security,
2: Securing and Managing Our Borders,
3: Enforcing and Administering Our Immigration Laws,
4: Safeguarding and Securing Cyberspace
5: Ensuring Resilience to Disasters.

C.1.4 CURRENT IT/NETWORK ENVIRONMENT

The following general network service groupings are currently offered by the DHS OCIO:

- Network and common enterprise applications at the SECRET level– the Homeland Secure Data Network (HSDN);
- Network and common enterprise applications at the TS/SCI level – the "C-LAN";
- Voice and video telecommunications;
- Unclassified voice and video telecommunications; and
- Unclassified Sensitive but Unclassified (SBU) network and common enterprise applications – the "A-LAN".

The Homeland Secure Data Network (HSDN) is the most mature network in the Department from the standpoint of offering managed enterprise-wide network services. It has been designed and implemented to provide common services to the DHS SECRET level community and its partners through standardized, certified and accredited endpoint Local Area Network (LAN) designs that deliver common enterprise applications, over, a common secure transport service, in support of the DHS mission. The certified and type-accredited designs apply to LAN sites with 20 or fewer devices, as more than 20 devices require enough individually detailed review to the point where they cannot be type-accredited.

HSDN consists of two sets of fully redundant core infrastructures of routers, servers, and data storage located at the two DHS Data Centers and connected by DHS' wide area network (OneNet). It also includes two redundant DMZ gateways to other SECRET networks (e.g., the Department of Defense SIPRNet), a Network Operations Center, a Security Operations Center, a helpdesk, the backbone network to connect the end user nodes, and the networked components at those nodes including the end point routers, servers, encryptors, workstations, printers, other peripheral equipment and services that operate on the network. Those enterprise services include email, organizational messaging Secure Video Teleconferencing (SVTC), a web portal, collaboration tools, applications hosting services, global backup and recovery services, and standard office automation tools. HSDN offers several standard end point configurations including, type-accredited small sites, type-accredited medium sites and custom large sites. In addition, HSDN also offers Secure Mobile Environment Portable Electronic Devices (SME-PEDs). This task order provides for the sustainment, operations, maintenance and incremental deployment of HSDN.

The DHS C-LAN provides current DHS HQ capabilities for TS and TS/SCI communications. C-LAN is a DHS managed extension of the Joint Worldwide Intelligence Communications System (JWICS). In a manner similar to HSDN, C-LAN also offers type-accredited small and medium sites, and a similar opportunity to define custom large sites. C-LAN is certified and accredited by the NSS CISO.

This task order provides for sustainment, operations, maintenance and incremental deployment of the C-LAN.

The Homeland TOP SECRET/SCI Network (HTSN) is supported in President's Budget for FY11. HTSN will streamline and modernize the DHS TS/SCI data capabilities to enhance TS/SCI data communications and collaboration within DHS and among DHS and other federal agencies and organizations, including the DoD and the Intelligence Community (IC). This service will strengthen both the TS/SCI data exchanges with the Department and with users of other networks. It will provide a scalable infrastructure, capable of supporting growth and evolution of the DHS mission. Until the HTSN architecture is defined, designed, implemented, tested and deployed, the current baseline C-LAN will be maintained and evolved appropriately.

Homeland Secure Communications (HSC) is a planned new program in DHS that will consolidate the planning, architecture, and implementation of secure voice and secure video communications into a centrally governed and managed activity. Motivated by the same opportunities to improve effectiveness and efficiency recognized in other aspects of networked services, HSC will provide effective and efficient voice and video services while saving considerable costs through leveraging common architecture, design, shared management, and leveraged investments.

DHS policy is driving migration to the common use of the infrastructures. Both HSDN and CLAN are each leveraging the common enterprise infrastructure elements as a foundation for heir service offerings.

C.1.4.1 EXTERNAL INTERDEPENDENT PROGRAMS

The following lists the external interdependent organizations and networked services that interface with DHS Enterprise Networked Services.

- OneNet is the DHS Wide Area Network (encrypted) composed of Verizon/AT&T leased circuits. Customs and Border Protection (CBP) is the steward for OneNet, which itself is a transition from an older Multiprotocol Label Switching (MPLS) network infrastructure. Management of OneNet is not within the scope of this task order;
- Data Centers 1 and 2 (DC1 and DC2), located in Mississippi and Virginia respectively, are established to consolidate information technology systems and to serve as backups for each other to maintain operations of critical departmental IT systems. Currently, the HSDN resides at both DC1 and DC2. The C-LAN resides at the Nebraska Avenue Complex (NAC) with a backup at DC2. Management of the infrastructure at the primary locations are within the scope of this task order, but management of the Data Centers themselves is not within the scope of this Task Order;
- SIPRNET is the Department of Defense networked infrastructure to transmit information up to and include information classified SECRET. DHS maintains an interface between the HSDN and the SIPRNET (only the management of the interface to the SIPRNET is within the scope of this task order);
- JWICS is the Intelligence Community's networked infrastructure for TS and TS/SCI connectivity. Management of only the interface to the JWICS is within the scope of this task order). C-LAN is an extension to the JWICS and maintains interfaces to it; and

- Director of National Intelligence – SECRET (DNI-S). For example, in the future, this may migrate into the planned Federal SECRET Fabric.
- Office of the Director of National Intelligence (ODNI) and Intelligence Community (IC) partners.
- In the future, enterprise networked services from other agencies (international, Federal, State, Local, and Tribal) may interface to DHS systems, services, and networks.

C.2 SCOPE

The scope of this task order includes design, engineering, architecture, integration, configuration, testing, deployment, sustainment, operations, and maintenance of the enterprise networked services. The scope also includes all of the above activities applied to the future successor system to C-LAN (known as the HTSN), HSC systems and additional systems identified in greater detail below

C.3 OBJECTIVE

The objective of this task order is to provide secure, enterprise networked services among DHS intelligence components, law enforcement agencies, emergency preparedness and response components, and other field activities for the purpose of moving data in support of DHS overall missions.

C.4 TASKS

Task 1: Task Order Management
Task 2: ENNS Operations and Maintenance, and Enhancement
Subtask 1: Systems Engineering, Architecture, and Technical Analysis
Subtask 2: Design, Development and Test
Task 3: HSDN Deployment
Task 4: C-LAN Deployment
Task 5: HTSN Development, Deployment and Sustainment (Optional)
Task 6: HSC Development, Deployment and Sustainment (Optional)
Task 7: Communications Security (COMSEC) Equipment, Policy, and Procedures
Task 8: Security Services

Task 9: Other IT Services
- **Subtask 1:** Video Conferencing
- **Subtask 2:** IT Continuity Management
- **Subtask 3:** Continuity Planning
- **Subtask 4:** Continuity Reviews and Coordination
- **Subtask 5:** Continuity Program Administration
- **Subtask 6:** Electronic Records

C.4.1 TASK 1 – TASK ORDER MANAGEMENT

The contractor shall provide task order management support services to efficiently manage the initial transition, the continuous evolution and the routine maintenance of DHS Enterprise Networked Services.

C.4.1.1 SUBTASK 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this Task Order. This includes the management and oversight of all activities performed by contractor personnel, including the effective use of subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a Program Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership for the execution of this task order.

C.4.1.1.1 COORDINATE A PROGRAM KICKOFF MEETING

The contractor shall schedule, coordinate and provide an agenda for a Program Kick-Off Meeting at a location approved by the Government. The meeting will provide an introduction between contractor personnel and Government personnel who will be involved with the task order. The meeting will provide an opportunity to discuss technical, management, security issues, travel authorization and reporting procedures. At a minimum, the attendees shall include key contractor personnel, DHS representatives, other relevant Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR).

The contractor shall provide the following at the kickoff meeting:
- Transition In Plan;
- Project Management Plan;
- Final Quality Control Plan; and
- Earned Value Management (EVM) Plan.

C.4.1.1.2 TRANSITION IN

The contractor shall ensure that there will be minimum service disruption to National Security Systems and no service degradation during and after transition. See H.27, Transition-In**,** for requirements.

C.4.1.1.3 STATUS REPORTS

C.4.1.1.3.1 WEEKLY ACTIVITY REPORT (WAR)

The contractor shall prepare a weekly activity report which is focused on operational issues.

The WAR shall include the following:

- Changes in the operational characteristics of all internal and external systems, subsystems, configurations, and services.
- Internal and external risks and issues
- Changes in program and project status
- All security issues (personnel, facility, events, incidents, and operational)

C.4.1.1.3.2 MONTHLY STATUS REPORT (MSR)

The contractor Program Manager shall develop and provide a MSR using MS Office Suite applications (Excel for numeric tables), within 15 working days after close of the contractor's accounting system, which includes the first of previous month through last day of previous month, via electronic mail to the Client Representative (CR) and the COR.

The MSR shall include the following:

- Activities during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task;
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them;
- Personnel gains, losses and status (security clearance, etc.);
- Government actions required;
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each);
- Summary of trips taken, conferences attended, etc.
- EVM statistics as applicable.

.

C.4.1.1.3.3 WEEKLY PROJECT REPORT (WPR)

For each active project, the contractor shall prepare a weekly project report which is focused on project status. This status shall be a weekly snapshot of real-time reports from a project execution management system. Industry Best Practices (e.g. PMBOK) for project execution and control shall be used.

The WPR shall include the following:

- Schedule Assessment Report identifying the likelihood of meeting target due date with projected completion date with schedule analysis (baseline and current, including progress along the critical path adjusted for resource constraints when appropriate);
- Milestone Status Report showing completions and general progress, identifying the current task on the critical chain (on which if no progress is made amounts to a day for day slip);
- Escalation Report to identify all outstanding issues (new, ongoing, and closed within last period) and the help needed to get the project back on track;
- Portfolio Management Report showing the amount of project schedule risk by customer, project size, or other; and
- Pipeline Management Report showing the flow of projects (approved and notional) showing the best utilization of critical resources, filling empty slots as priority allows.

C.4.1.1.4 EARNED VALUE MANAGEMENT (EVM) CRITERIA

The contractor shall employ and report on EVM in the management of this Task Order. See H.19, Earned Value Management**,** for the EVM requirements.

C.4.1.1.5 CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager shall convene a monthly Task order Activity and Status Meeting with the CR, COR, and other vital government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor Program Manager shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five calendar days following the meeting.

C.4.1.1.5.1 PROGRESS MEETINGS

The Program Manager shall be available to meet with the COR and/or CR upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. These meetings may take place at FEDSIM, a DHS facility in the Washington DC Metropolitan Area or via teleconference.

C.4.1.1.5.1 Integrated Baseline Reviews

The Contractor shall conduct a post award Integrated Baseline Review (IBR). The Government may require additional IBRs at the exercise of significant options or the incorporation of major modifications.

C.4.1.1.6 PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP.

The PMP shall:

- describe the proposed management approach;
- contain detailed Standard Operating Procedures (SOPs) for all tasks;
- include milestones, tasks, and subtasks required in this task order;
- provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations; and
- include the contractor's Quality Control Plan (QCP) and EVM Plan.

The contractor shall provide the Government with a draft PMP at the Kick-Off Meeting, on which the Government will make comment. The final PMP shall incorporate Government comments and shall be provided 30 calendar days after the Kick-Off Meeting.

C.4.1.1.6.1 PREPARE AND UPDATE WORK BREAKDOWN STRUCTURE

The contractor shall prepare and update the project WBS derived from the PWS and linked to the project schedule, budget, and time-phased expenditure plan. The WBS will be included as part of the PMP, will be available online, and will be maintained for the life of the task order.

The contractor shall use the WBS as a means of assigning responsibilities to project task leaders and, along with the detailed schedule and time-phased budget, tracking progress at the detailed task level. The WBS will be modified, as needed, to reflect changing project emphasis, or to provide better visibility and tracking of project activities.

C.4.1.1.6.2 PROJECT MANAGEMENT PLAN (PMP) UPDATES

The PMP is an evolutionary document that shall be updated, at a minimum, yearly. The contractor shall work from the latest Government approved version of the PMP.

C.4.1.1.7 PREPARE DETAILED TRIP REPORTS

The contractor shall provide detailed trip reports at Government request prior to MSR delivery, which include the following: by trip, the name of the employee, location of travel, duration of trip, trip costs (lodging, travel, per diem) Reports as requested are due ten (10) business days after trip completion. All other trip reporting, shall be via the Monthly Status Reports as described in paragraph C.4.1.1.3.2.

Site surveys and deployments will be documented in the site install plan (draft/final). Site survey and deployment cost will be individually documented in the monthly RFC summary report (a subset of the monthly invoice).

C.4.1.1.8 UPDATE QUALITY CONTROL PLAN (QCP)

The contractor shall update the QCP submitted with their proposal and provide a final QCP five (5) days after task order award. The contractor shall update the QCP (minimum of yearly) to reflect changes in the plan.

C.4.1.1.9 BUSINESS CONTINUITY PLAN (BCP)

The Contractor shall prepare and submit a BCP to the Government. The BCP Plan shall be due 30 days after task order date of award, and shall be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism.

The BCP, at a minimum, shall include the following:

- A description of the Contractor's emergency management procedures and policy;
- A description of how the Contractor will account for their employees during an emergency;
- How the Contractor will communicate with the Government during emergencies; and
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
    - Telephone numbers and
    - E-mail addresses

Individual systems described within the BCP shall be activated immediately after determining that an emergency has occurred, shall be operational within eight (8) hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the task order is terminated, whichever comes first. In case of a life threatening emergency, the CR shall immediately make contact with the Contractor Program Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency.

When any disruption of normal, daily operations occur, the Contractor Program Manager and the CR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and contractor);
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.);
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.); and
- Essential Contractor work products expected to be continued, by priority.

The Government and Contractor Program Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. The contractor shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this task order.

C.4.1.1.10 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all EIT products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. The contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

- 36 CFR 1194.21 - Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including to Government developed and owned software and hardware (GOTS) and Commercial off the Shelf (COTS) software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

- 36 CFR 1194.22 - Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as Flash or Asynchronous JavaScript and XML (AJAX) then "1194.21 Software" standards also apply to fulfill functional performance criteria.

- 36 CFR 1194.23 - Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

- 36 CFR 1194.24 - Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

- 36 CFR 1194.25 - Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.

- 36 CFR 1194.26 - Desktop and Portable Computers, applies to all desktop and portable computers, including laptops and personal data assistants (PDA) that are procured or developed under this work statement.

- 36 CFR 1194.31 - Functional Performance Criteria applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

- 36 CFR 1194.41 - Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required "1194.31 Functional Performance Criteria", they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied.

Any request for additional exceptions shall be sent to the CR and determination will be made in accordance with DHS MD 4010.2.

DHS has identified the following exceptions that may apply:

- 36 CFR 1194.2(b) - (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards.

  When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected

product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

- 36 CFR 1194.3(b) - Incidental to Task order, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

- 36 CFR 1194.3(f) - Back Office, applies to any EIT item that will be located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment. This exception does not include remote user interfaces that are accessible outside the enclosed "space".

- EXEMPTION FOR NATIONAL SECURITY SYSTEMS.--This section shall not apply to national security systems, as that term is defined in section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452):

  (a) DEFINITION- In this subtitle, the term `national security system' means any telecommunications or information system operated by the United States Government, the function, operation, or use of which--

  (1) involves intelligence activities;
  (2) involves cryptologic activities related to national security;
  (3) involves command and control of military forces;
  (4) involves equipment that is an integral part of a weapon or weapons system; or
  (5) subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions.

  (b) LIMITATION- Subsection (a) (5) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

C.4.1.1.11 IMPLEMENT TRANSITION OUT PLAN

The contractor shall implement its Transition-Out Plan no later than 120 calendar days prior to expiration of the task order. See Section H.28, Transition Out for additional information.

C.4.1.2 CHANGE MANAGEMENT PROCESS

The contractor shall provide a process to manage all changes to enterprise networked services. The contractor shall prepare and deliver a Configuration Management Plan (CMP) to provide process detail which supports this requirement. This process shall be driven by Requests for Change (RFC), with a formal submission and approval processes that integrate with DHS' Department-wide change management authorities (e.g. Enterprise Architecture Center of Excellence (EACOE), Infrastructure Configuration Control Board (ICCB), NSS Accreditation Working Group (NSSAWG)) and existing governance mechanisms. This process shall be implemented by an electronic work flow control system. The financial management process for this task order shall be integrated with this electronic workflow control system and all reports which that process generates. The entire CM process shall feed the online electronic project status reporting requirement specified in C.4.1.1.3.3.

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and/or software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

The contractor shall adhere to a controlled mechanism for keeping both costs and schedule within the following bounds: to the extent where the contractor has control over the activities in the change process, costs and schedule actual performance is required to not vary by more than +5% and -10% of estimates which are provided in the RFC. The purpose of this control mechanism is to ensure accuracy in cost and schedule estimation.

C.4.2 TASK 2 –ENSS OPERATIONS, MAINTENANCE AND ENHANCEMENT

The contractor shall provide design, engineering, architecture, integration, configuration, testing, deployment, sustainment, operations, and maintenance. This task order will provide services which enhance and integrate with the DHS Network Operations Center, Security Operations Center, Headquarters Operations Center (HOC), Helpdesk and desk side support in accordance with the Service Level Agreements (SLAs).

The contractor shall:

a. Provide all of the technical services necessary to engineer, operate, deploy, and maintain the networks for DHS;

b. Provide services in accordance with the Service Level Agreements (SLAs) as outlined in Section J, Attachment E;

c. Provide operations and maintenance of networks, including the following;

- Monitoring and reporting in real- and near real-time all enterprise networked services for operational status and utilization,
- Operate 24x7 Network Operations Centers (NOC),
- Operate 24x7 Helpdesk Support,
- Manage and coordinate circuit provisioning with the designated circuit management personnel,
- Maintain configuration management database,
- Manage and maintain secure radio frequency (RF) and non-radio frequency wireless communications (e.g. SME-PED, Land Mobile Radio (LMR), laser, and SATCOM),
- Provide Secure Messaging System (SMS) administration and support,
- Manage End-user account processing (e.g. create, modify and delete),
- Provide training to end users and site administrators,
- Provide desktop support and customer follow-up,
- Provide preventive maintenance and obsolescence management, and
- Make recommendations for improved services.

d. Perform project control activities and performance management report for all projects and sites including;

- Scheduling Activities,
- Request for Change (RFC) support as it relates to operations and maintenance activities, and
- Business Administration support.

e. Provide remote operations and management as well as on site maintenance as required for systems hosted at data centers;

f. Develop an access management procedure with the DHS Data Center contractor;

g. Manage and operate remote network user login services;

h. Prepare Rough Order Magnitudes, technical drawings and explanations, presentation materials, and provide subject matter expertise as needed to promote approval and implementation of RFCs;

i. Maintain, monitor and manage the DHS Enterprise Networked Services infrastructure;

j. Provide performance tuning and optimization services;

k. Perform evaluation and verification of deployments and system upgrades;

l. Maintain specialized user applications and database requests;

m. Verify installed configurations are consistent with configuration management and version control of all software, privileged and normal user accounts; and

n. Perform Information Technology Information Library (ITIL) Capacity Management processes to ensure that all serviced elements are provisioned to support operational SLAs.

C.4.2.1 SUBTASK 1 – SYSTEMS ENGINEERING, ARCHITECTURE, AND TECHNICAL ANALYSIS

The contractor shall develop, and upon Government approval, execute a technical strategy to sustain and improve enterprise networked services in a disciplined and structured manner.

The contractor shall:

a. Ensure architecture, engineering, and design of networked services are consistent with DHS standards, regulations, policies and approved practices;

b. Documenting the operational user requirements and the technical system derived requirements in preparation for system design, i.e. document, and manage end user and business owner operational requirements, key performance attributes, and measures of effectiveness for infrastructure systems functionality;

c. Maintain the technical as-built documentation of the infrastructure;

d. Maintain the “To-Be” architecture and build-out plan to a level of granularity that enables trade-off analysis to be performed that supports annual and special program planning and budgeting exercises;

e. Develop engineering solutions for the continuous improvement of DHS Enterprise Networked Services;

f. Review and evaluate proposed engineering and architectural solutions and submit recommended solutions for Government approval;

g. Develop Rough Order of Magnitude (ROM)/RFC Development for service requests to meet Components and user requirements, based on processes that are defined by the Configuration Management Plan (CMP);

h. Develop and update documentation in accordance with DHS Acquisition Directive 102-01 and the Systems Engineering Life Cycle (SELC);

i. Provide technical and engineering services for network changes and enhancements;

j. Provide engineering solutions to the information sharing problem which involve the deployment of cross domain solutions; and

k. Provide engineering solutions which address all aspects of enterprise management (networks, services, and applications). Provide interface solutions to enterprise services provided by external organizations.

C.4.2.2 SUBTASK 2 – DESIGN, DEVELOPMENT AND TEST

The contractor shall design, develop, acquire, implement, integrate, test, document, and secure systems and subsystems with the objective to provide reliable, available, and secure data transport; and application hosting and access for authorized users.

The contractor shall:

a. Provide development laboratory environments at Government-provided locations or at contractor-provided locations that are approved by the Government which are capable of simulating or replicating conditions on the operational network, isolated from ongoing operations;

b. Operate, maintain and provide timely refreshes as technology evolves;

c. Provide all management and logistics support for engineering services functions in compliance with DHS standards and policies;

d. Develop and execute strategies and plans for interfacing to or incorporating currently independent operational enclaves;

e. Develop and track the allocation of operational requirements to the system design level, including technical systems, manpower, resources, operations and logistics;

f. Demonstrate that system level requirements are reflective of end user and business owner operational requirements;

g. Maintain requirements traceability throughout the lifecycle;

h. As required and approved, provide operations and management of applications. DHS uses a combination of Commercial Off the Shelf (COTS), Government Off the Shelf

(GOTS) and custom developed applications to support specific missions in the Department;

i. Provide development to customize applications to operate in mission scenarios and provide application support to maintain and extend mission application capabilities;

j. Provide advice on emergency radio communications that interface with DHS computer networks, develop solution plans, and implement as directed;

k. Assess and provide options for how interoperability across these systems can be enhanced;

l. Implement identity, credentialing, and access management services consistent with DHS Policies and Procedures;

m. Identify, acquire, customize and integrate the suite of technical management tools required to control communication network priorities so that secure video-teleconferencing (SVTC) and voice over secure IP (VoSIP) operate at a level of quality of service (QoS) appropriate to the successful implementation of these capabilities;

n. Establish and support remote network user login services;

o. Design and develop a methodology and mechanism for performance optimization of enterprise networked services;

p. Develop and update systems engineering documentation in accordance with DHS SELC policy and guidelines;

q. Assist the government in evolution of standardized business processes consistent with ITIL;

r. Across all enterprise networked services, use a standardized, consistent, and disciplined approach for all systems engineering, architecture, design, development, integration, security, deployment, testing, operations, and maintenance activities;

s. In accordance with the RFC process, design and develop new system capabilities and repair problems identified during discovery or reported by end users and support personnel;

t. Apply standardized and consistent systems engineering methods to every RFC to ensure that reliability, availability, and security of the enterprise is maintained without introduction of unacceptable risk;

u. Prepare Rough Order Magnitude estimates, technical drawings and explanations, and presentation materials, as needed to support approval and implementation of RFCs; and

v. Develop training packages for all users and administrators.

C.4.3 TASK 3 – HSDN DEPLOYMENT

The contractor shall acquire, warehouse, inventory, transport, install, configure, integrate, test, and secure components of the HSDN for deployment to new and existing sites. The contractor shall develop and present standard training modules to authorized users and administrators.

The contractor shall:

a. Ensure that work on all approved site Move, Add or Change (MAC) requests comply with the DHS network and enterprise architecture, DHS policy and guidance documents, and with all pertinent security requirements;

b. Provide project tracking of all RFCs. Produce Rough Order of Magnitude estimates for schedule, costs, and technical requirements (For Example: Evaluate physical, electrical, HVAC, circuit and security capabilities/characteristics, etc) to satisfy RFCs, including MACs, service enhancements, and deployments;

c. Execute deployment, moves, additions or changes in accordance with approved RFCs;

d. Plan, develop and document all requirements for HSDN deployments and prepare cost and schedule estimates in support of RFC submissions;

e. Provide turn-key services to create or modify existing or new IT facilities approved for the installation and operation of systems, including SECRET and TOP SECRET /SCI at the customer location specified in each RFC;

f. Provide positive physical control of warehouse inventory, databases enumerating that inventory, and access control by project personnel to the equipment warehouse, in accordance with Federal policies for handling of classified material;

g. Provide support for RFC presentation and review by the ERB and CCB and delivery to the DHS;

h. Provide all of the technical services necessary to deploy new sites, and to do moves/adds/changes to existing sites based on approved RFCs;

i. Provide logistical support to meet the deployment standards defined by the SLAs; and

j. Develop and present training to end users and site administrators.

C.4.4 TASK 4 – C-LAN DEPLOYMENT

The contractor shall acquire, warehouse, inventory, transport, install, configure, integrate, test, and secure components of the C-LAN for deployment to new and existing sites. The contractor shall develop and present standard training modules to authorized users and administrators.

The contractor shall:

a. Ensure that work on all approved site Move, Add or Change (MAC) requests comply with the DHS network and enterprise architecture, DHS policy and guidance documents, and with all pertinent security requirements;

b. Provide project tracking of all RFCs. Produce Rough Order of Magnitude estimates for schedule, costs, and technical requirements (For Example: Evaluate physical, electrical, HVAC, circuit and security capabilities/characteristics, etc) to satisfy RFCs, including MACs, service enhancements, and deployments;

c. Execute deployment, moves, additions or changes in accordance with approved RFCs;

d. Plan, develop and document all requirements for C-LAN deployments and prepare cost and schedule estimates in support of RFC submissions;

e. Provide turn-key services to create or modify existing or new IT facilities approved for the installation and operation of systems at the TOP SECRET /SCI customer location specified in each RFC;

f. Provide positive physical control of warehouse inventory, databases enumerating that inventory, and access control by project personnel to the equipment warehouse, in accordance with Federal policies for handling of TS/SCI material;

g. Provide support for RFC presentation and review by the ERB and CCB and delivery to the DHS;

h. Provide all of the technical services necessary to deploy new sites, and to do moves/adds/changes to existing sites based on approved RFCs;

i. Provide logistical support to meet the deployment standards defined by the SLAs; and

j. Develop and present training to end users and site administrators.

C.4.5 TASK 5 – HTSN DEVELOPMENT, DEPLOYMENT AND SUSTAINMENT (OPTIONAL)

The contractor shall provide a responsive, reliable, survivable computing infrastructure platform and framework for voice, video and data communications in support of TS/SCI collaboration, information sharing, and knowledge management activities across DHS and its homeland security partners.

The contractor shall:

a. Perform design, acquisition, testing, integration, deployment and transition activities to implement the following features:

- A centrally governed enterprise-level TS/SCI network that accommodates existing and future DHS network circuits;
- A potential future TS collateral network
- Common provisioning of enterprise applications to include office productivity, file sharing, and email;
- An infrastructure capable of hosting existing and current and future intelligence applications;
- A central network and security operations and monitoring capability;
- Conventional and low-cost type accredited workstation solutions, WAN and communication interface designs;
- Critical backup, recovery, and Continuity of Operations (COOP) capability

a. Provide development laboratory environments at Government-provided locations or at contractor-provided locations that are approved by the Government which are capable of simulating or replicating conditions on the operational network, isolated from ongoing operations.

C.4.6 TASK 6 – HSC DEVELOPMENT, DEPLOYMENT AND SUSTAINMENT (OPTIONAL)

Leveraging existing DHS components and networks, the contractor shall provide the voice, video, and data communications infrastructure and supporting operations necessary to exchange national security information for intelligence sharing and analysis; counterterrorism planning; and crisis response across DHS and its homeland security partners.

The contractor shall perform design, acquisition, testing, integration and deployment activities to implement the following capabilities:

a) Virtual Collaboration to include;

- Hosting conferences with multiple participants (DHS Components, other Federal agencies, and State and local homeland security partners),

- Voice and video collaboration with document sharing and data streaming (video, satellite feeds),

- Desktop-based point-to-point Video Teleconferencing (VTC),

- Voice-only devices, and

- Connection to classified VTC and Collaboration sessions using Secure Telephone Equipment (STE) and secure wired and wireless devices,

b) Mobile Communications, to include;

- Wireless (satellite and cellular) communications (includes email and internet access), in Continental United States (CONUS) and Outside the Continental United States (OCONUS),

- Connectivity among mobile classified mobile communications devices, remote operations centers, and the DHS communications infrastructure,

- Connectivity to field operators,

    - In CONUS along the US Borders, airfields and other ports of entry, and
    - In remote locations (including OCONUS),

- Communications relay between mobile radios via IP over landlines,

- Deployable communications centers,

- Interoperability between DHS mobile devices and other federal agencies' (e.g. the White House) in-house communications devices, and

- Directory Services.

C.4.7 TASK 7 – COMMUNICATIONS SECURITY (COMSEC) EQUIPMENT, POLICY, AND PROCEDURES

- Utilize the DHS COMSEC Material Control System (CMCS) for the distribution, deployment, and accountability of COMSEC materials and equipment;

- In accordance with DHS Management Directive 4300B, augment and assist with the operation and maintenance of the DHS National COMSEC account and the DHS National Capital Region COMSEC account for distribution and accountability of COMSEC materials and equipment;

- Incorporate and develop engineering solutions to facilitate the Electronic Key Management System (EKMS) and the future Key Management Infrastructure (KMI) into the system architecture for deployment of electronic key to enterprise networked encryption equipment;

- Procure, warehouse, control, and deploy all Controlled Cryptographic Items (CCI) through the DHS National COMSEC accounts IAW approved Requests for Change (RFCs) and the approval of the DHS COMSEC Central Office of Record.

C.4.8 TASK 8 – SECURITY SERVICES

The contractor shall support management of the security processes, controls and tools that provide information assurance among the enterprise networked services, in accordance with DHS Management Directive 4300B and DCID 6/3. The contractor shall support the DHS Risk Management Division (RMD) in their oversight of security compliance of HSDN and C-LAN systems relative to DHS security policies, guidance and mandates.

The contractor shall provide engineering, operations, and maintenance of functions necessary to provide all security solutions and services for the DHS security compliance program, to include:

- Operate 24x7 Security Operations Centers (SOC) to include continual security monitoring of all relevant systems to track potentially suspicious anomalies, and analyze these anomalies to determine whether they are reportable security events,

- All security events and notification will be reported to the enterprise DHS SOC and relevant parties for escalation,

- Ensure compliance through development and maintenance of sufficient security controls, processes and procedures to meet DHS Information Assurance, Information Security, and Communications Security policies and procedures,

- Conduct continual security scans, perform analysis of the scan results, and report all findings,

- Support response to all security events on the HSDN and C-LAN, including developing Incident Response Plans, taking remediation actions, and coordinating with other incident responder organizations,

- Support disaster recovery and contingency planning activities

- Provide security training to end users and site administrators,

- Make recommendations for improved security services.

    a. Develop and maintain all relevant security documentation including C&A Updates, Security Incident Reports, Standard Operating Processes and Procedures as well as other documentation in accordance with the DHS SELC;

    b. Change Management

- Perform validation and remediation of all proposed changes to maintain or enhance existing security controls, processes or procedures.

- Ensure that all proposed changes are processed in accordance with the CMP for appropriate approval and guidance.

c. Patch Management

- Monitor and report on the timeliness of implementation of patches to mitigate security risks and findings,

- Provide patch management and reporting of security risks and findings, and

- Perform patch and upgrade management.

The contractor shall provide engineering functions necessary to provide all security solutions and services for the DHS security compliance program, to include:

a. Provide security engineering support in close coordination with enterprise engineering functions within this Task Order and in compliance with the Configuration Management Plan, to include:

- Engineering assistance to develop modifications that implement technical security policies and controls, consistent with DHS Enterprise Architectures, policies and standards;

- Integrate security processes, controls and technologies into technical solutions.

- Where feasible, leverage type-accredited solutions, and a consistent approach in design, development, and testing;

- Develop situation-specific, accreditable solutions;

- Provide a comprehensive assessment of the security posture and vulnerability of newly engineered IT services, as required;

- Develop engineering solutions to correct anomalies identified during periodic security testing, while ensuring certification and accreditation is maintained;

C.4.9 TASK 9 – OTHER IT SERVICES

The contractor shall provide Other IT Services and maintenance in accordance with the Service Level Agreements (SLAs).

C.4.9.1 SUBTASK 1 – VIDEO CONFERENCING

The contractor shall:

- Engineer, operate, and maintain video teleconferencing and multimedia services and equipment. Conferencing and multimedia equipment includes support for secure and non-secure bridging systems, display and projection systems, electronic whiteboards, audio systems, DVD and video recording and replay, video switching systems, control systems, and video cameras;

- Provide 7x24x365 (366 for leap years) support for set up and operation of VTC and multimedia systems for selected DHS buildings (currently 2 locations but may increase over the life-cycle of the award); provide user level maintenance support for VTC and multi-media systems, and operate video conferences at multiple locations;

- Maintain, setup, monitor, and troubleshoot video equipment for users. The contractor shall assist customers with the use of video conferencing systems by providing personal instruction in the use of control interfaces and procedures;

- Schedule and monitor all video teleconferencing sessions;

- Maintain an inventory of video conferencing equipment owned and leased by DHS;

- Maintain a DHS video conferencing contact list;

- Maintain and operate a VTC management platform;

- Install, replace and configure video conferencing equipment required by DHS Component customers; and

- Complete all work at SECRET and TS/SCI.

C.4.9.2 SUBTASK 2 – IT CONTINUITY MANAGEMENT

The contractor shall:

- Perform continuity management actions affecting the Information Technology Service Office and all of its functions including the Network Management Center, Security Management Center, Front Office, Enterprise Business Management Office, Infrastructure Information Systems Security Manager (ISSM), Mission Critical Infrastructure Operations (MCIO), Enterprise Application Delivery and Operations, IT Continuity Management, Business Office Operations, Infrastructure Transformation Office, Wireless Management Office, and all network and telecommunications components;

- Provide continuity management and redundancy capability to the Help Desk;

- These programs/offices have recoverable IT essential functions (EFs) with alternate site operations occurring on the systems. Provide IT integration capability for all departmental, intergovernmental, and non-governmental organization (NGO) applications used on the networks.

C.4.9.3 SUBTASK 3 –CONTINUITY PLANNING

For the networks and systems, the contractor shall:

- Coordinate strategic planning with programs and offices annually. The outcome of the strategic planning is the Multi-Year Strategic Program Management Plan containing continuity planning goals and objectives to include performance measures for the period;

- Update and maintain annually the national security systems sections of the CIO COOP Implementation Plan. The contractor shall provide the document to the CR for approval;

- Develop, maintain, update and implement the Incident Response and Management Plan, containing management activist and emergency response and escalation procedures. The contractor shall update the plan annually based on threat, exposure and business continuity strategy; and

- Develop, maintain, update the national security system sections of the CIO Operational Recovery Plan and IT Disaster Recovery/Business Continuity Plans, at least annually for offices and programs.

C.4.9.4 SUBTASK 4 –CONTINUITY REVIEWS AND COORDINATION

For the networks and systems the contractor shall:

- Participate in Enterprise Architecture Center of Excellence (EACOE) reviews, Enterprise Change Control Board (ECCB) reviews, and other compliance activities to identify the impact of these bodies' decisions and actions on IT continuity planning and advise these bodies' on continuity planning considerations. The contractor shall document the reviews continuity planning impacts and provide comments in accordance with the guidelines provided by the appropriate board; and

- Schedule, plan and conduct a periodic meeting of designated stake holders to discuss and coordinate requirements for the development and maintenance of the Disaster Recovery and IT Contingency Plan and coordinate the plans and activities for conducting COOP Exercises. The meeting participants shall also coordinate actions taken to address findings resulting from COOP exercises. The contractor shall provide meeting minutes to the CR within three business days of the meeting.

C.4.9.5 SUBTASK 5 –CONTINUITY PROGRAM ADMINISTRATION

For the networks and systems, the contractor shall:

- Develop, maintain, update and implement IT continuity policy, guidance, methodologies and tools. Updates shall occur at least annually, in response to Homeland Security Presidential Directives (HSPDs), or as directed by the CR;

- Update and maintain the list of CIO essential functions and critical IT and telecommunication networks, systems, facilities, and critical positions;

- Perform a continuity management review, periodically, or when significant changes occur to the essential function(s) or DHS IT infrastructure. Changes shall result in a threat and vulnerability exposure, Risk Assessment, Interdependency Analysis, Business Impact Analysis. The contractor shall ensure re-use of existing information when performing the aforementioned tasks. The contractor shall prepare a report and executive briefing identifying risk to the CIO;

- Conduct a review of the CIO COOP Implementation program, Operational Recovery/IT Contingency Plans, observe related tests, and provide feedback on program compliance in accordance with all applicable executive orders, presidential directives, other federal and DHS laws, federal orders management policies, handbooks, guidelines, processes, and procedures; and

- Develop executive briefings.

C.4.9.6 SUBTASK 6–ELECTRONIC RECORDS

For the networks and systems, the contractor shall:

- Develop, maintain, update and implement the electronic vital records program to ensure critical records are stored off premise. Records range from paper-based documents to the latest electronic-storage media;

- Ensure off-site storage location(s) be located at least 50 miles from the production site, outside of the impact area of the production site, and inside the continental U.S.;

- The frequency of records back-up is dependent on the record type;

- The retrievable and fully operational time frames shall fulfill the performance requirements for critical and non-critical systems as identified in Continuity of Government Condition (COGCON) level activation and reconstitution timeframes; and

- Test and ensure the records are retrievable and usable at least quarterly. The contractor shall provide a test report to the CR within five (5) business days of completing the test.